

## Environment setup:

```
[10/20/21]seed@VM:~/../Labsetup$ dcbuild
Building elgg
Step 1/10 : FROM handsonsecurity/seed-elgg:original
--> e7f441caa931
Step 2/10 : ARG WWWDir=/var/www/elgg
--> Using cache
--> 10e7c2df34d4
Step 3/10 : COPY elgg/settings.php $WWWDir/elgg-config/settings.php
--> Using cache
--> da68e4647533
Step 4/10 : COPY elgg/Csrf.php      $WWWDir/vendor/elgg/elgg/engine/classes/Elgg/Security/Csrf.php
--> Using cache
--> b759d667b464
Step 5/10 : COPY elgg/ajax.js      $WWWDir/vendor/elgg/elgg/views/default/core/js/
--> Using cache
--> 7893fc9765d9
Step 6/10 : COPY apache_elgg.conf /etc/apache2/sites-available/
--> Using cache
--> aabe586c167c
```

## Building the docker server using dcbuild

```
[10/20/21]seed@VM:~/../Labsetup$ dcup
```

## Starting the server using dcup

```
10.9.0.5      www.seed-server.com
10.9.0.5      www.example32.com
10.9.0.105    www.attacker32.com
"/etc/hosts" 35L, 868C
```

Mapping the addresses in /etc/hosts for attacker, example and seed-server

## Task1:

The screenshot shows a web browser window with the address bar displaying `www.seed-server.com/search?q=alice&search_type=all`. The page title is "Elgg For SEED Labs" and the search results are for "alice". The results list includes a user profile for "Alice (@alice)".

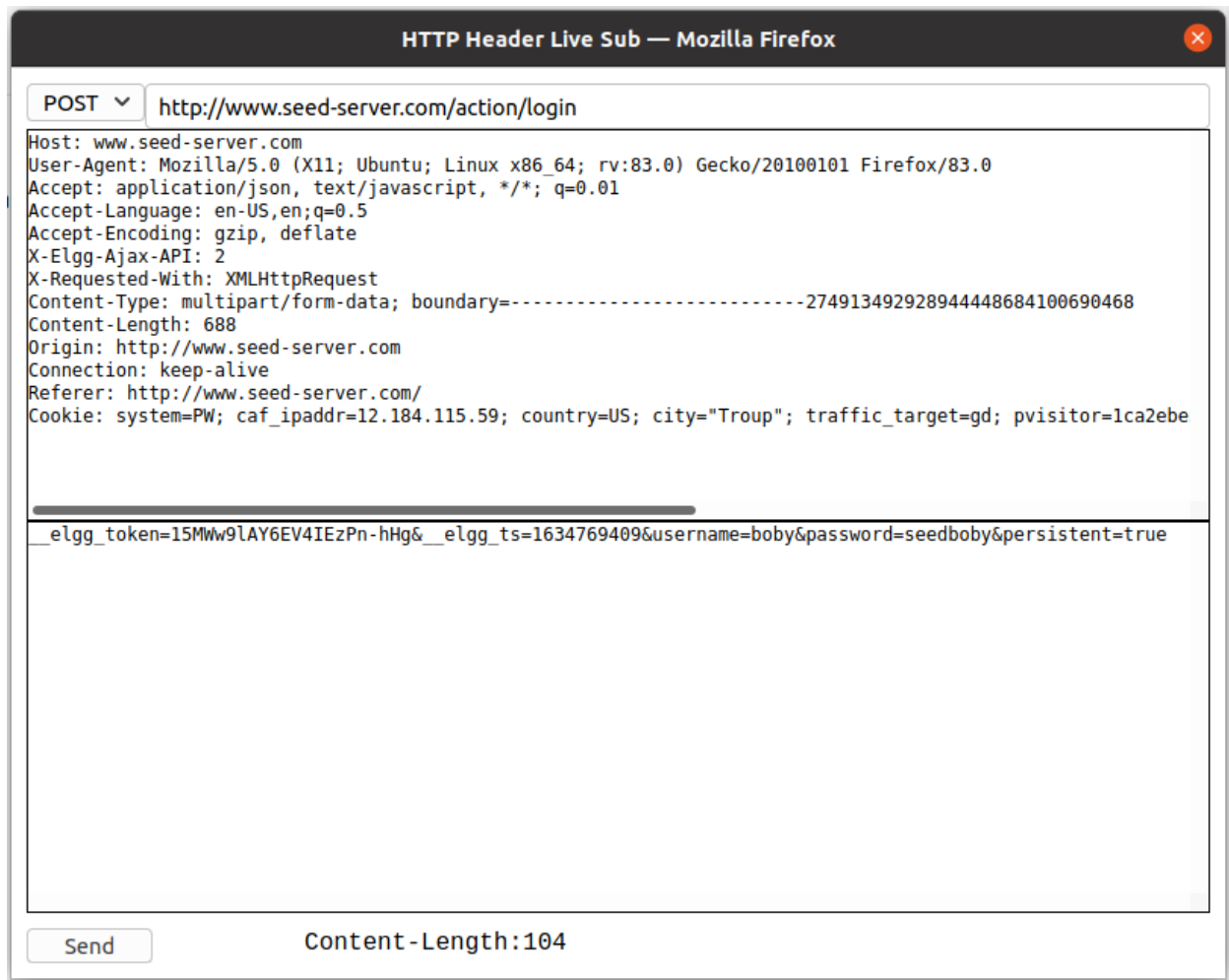
Overlaid on the page is the "HTTP Header Live" add-on window, which displays the following information:

- URL:** `http://www.seed-server.com/search?q=alice&search_type=all`
- Host:** `www.seed-server.com`
- User-Agent:** `Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/99.0`
- Accept:** `text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8`
- Accept-Language:** `en-US,en;q=0.5`
- Accept-Encoding:** `gzip, deflate`
- Connection:** `keep-alive`
- Referer:** `http://www.seed-server.com/blog/all`
- Cookie:** `system=PW; caf_ipaddr=12.184.115.59; country=US`
- Upgrade-Insecure-Requests:** `1`
- GET:** `HTTP/1.1 200 OK`
- Date:** `Wed, 20 Oct 2021 22:28:20 GMT`
- Server:** `Apache/2.4.41 (Ubuntu)`
- Cache-Control:** `must-revalidate, no-cache, no-store, private`
- Expires:** `Thu, 19 Nov 1981 08:52:00 GMT`
- Pragma:** `no-cache`
- X-Content-Type-Options:** `nosniff`
- Vary:** `Accept-Encoding, User-Agent`
- Content-Encoding:** `gzip`
- Content-Length:** `3616`
- Keep-Alive:** `timeout=5, max=100`
- Connection:** `Keep-Alive`
- Content-Type:** `text/html; charset=UTF-8`

The add-on window also shows a list of requests and responses, including the following details:

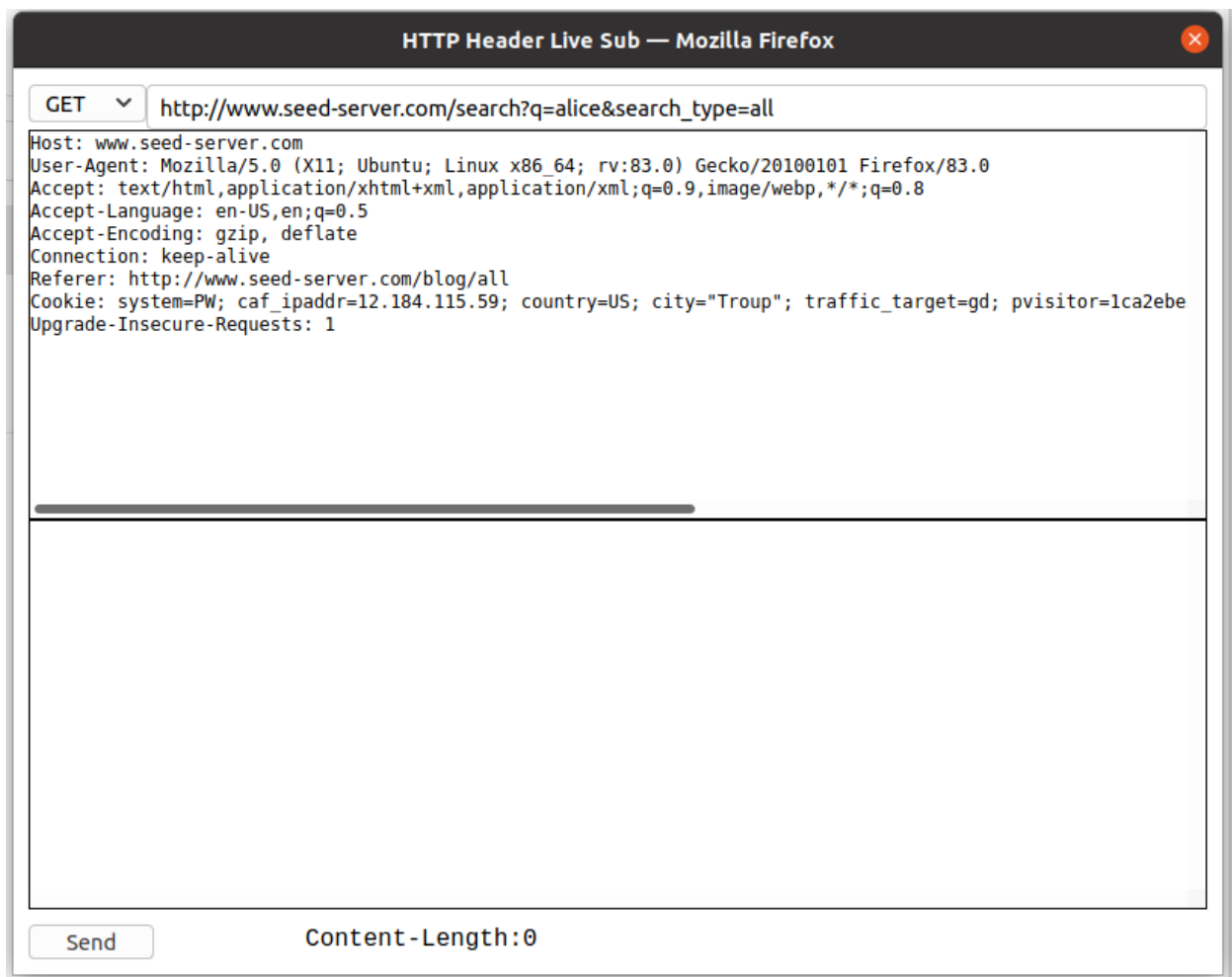
- Request:** `GET /search?q=alice&search_type=all HTTP/1.1`
- Response:** `HTTP/1.1 200 OK`
- Cache-Control:** `max-age=15552000, public, s-maxage=15552000`
- X-Content-Type-Options:** `nosniff`
- Etag:** `"1587931381-gzip"`
- Last-Modified:** `Wed, 20 Oct 2021 19:27:17 GMT`

Using HTTP header live add-on to track all the requests and responses in the webpage



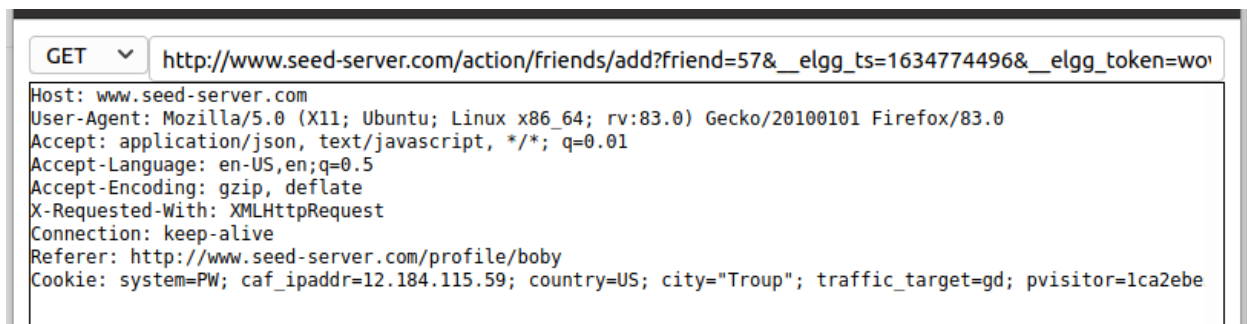
We use the HTTP header live tool to capture a HTTP post request being sent to elgg website

The post request has a body to it, which is used to sent along with the post request the elgg server



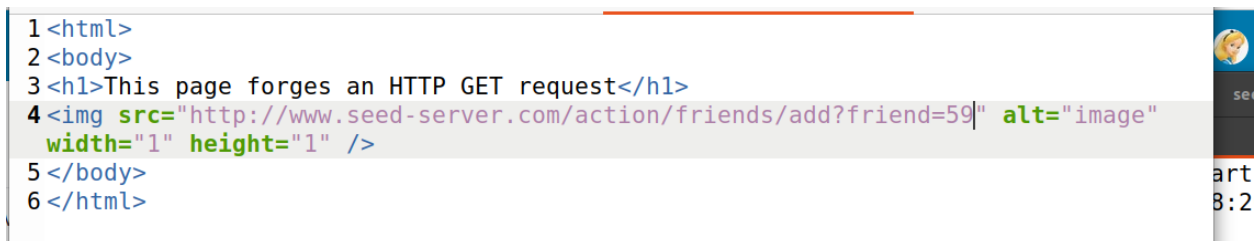
Here We use the HTTP header live tool to capture a HTTP get request being sent to elgg website  
And the HTTP get request is used to get the requested data from the server

## Task2



Here we use HTTP get request to get the url for our attack which can be seen in the src part of the next image

`'owner_guid':59,` this is the id for samy which we get from the source page of samy's profile



Restart server and we have got the friend id from the guid of samy and the url by using add friend button using the http header live which we see in the above image

## Log in

Username or email \*

samy|

Password \*

.....

☐ Remember me

Log in

[Lost password](#)

Login as samy so that we can set up the attack



Blogs

Bookmarks

Files

Pages

Wire post

About me

open my profile for free miracles. we can be good firends image

 [Add widgets](#)

Title \*

this is new one open for good vibe

Excerpt

Body \*

B

I

U

S

T<sub>x</sub>

Embed content

Edit HTML

http://www.attacker32.com/addfriend.html

Samy

Blogs

Bookmarks

Files

Pages

Wire post

Samy writes a post that has the attacker website and publishes it on the blog so that alice can open it when she sees it

this is new one open for good vibe

By Samy

🕒 just now

🌐 Public

💬

👍

⋮

<http://www.attacker32.com/addfriend.html>

⏪ Previous

Comments

Embed content

Edit HTML

B

I

U

S

T<sub>x</sub>

Here is the preview of the post that Sammy created

Alice's friends

No friends yet.

Alice

Blogs

Bookmarks

Files

Pages

Wire post

Here we login as alice and see that she has no friends right now

Samy » Blogs

## this is new one open for good vibe



By Samy 37 minutes ago Public



<http://www.attacker32.com/addfriend.html>

« Previous

### Comments

[Embed content](#) [Edit HTML](#)

B I U S T<sub>x</sub>



Samy

Blogs

Bookmarks

Files

Pages

Wire post

Alice reads samy's post and opens the url which redirects alice to the melecious website (here the get request is being forget) where our attack runs which make our attacker (samy) friend to anyone who views the website being logged in

← → ↺ 🏠 [www.attacker32.com/addfriend.html](http://www.attacker32.com/addfriend.html)

## This page forges an HTTP GET request

This is the malicious website preview

### Alice's friends



Samy



Alice

Blogs

Bookmarks

Files

Pages

Wire post

When we see alices's friend list after the attack is done, we can see that samy is now friend to alice



### Task3:

The screenshot shows a web browser with three tabs: 'Assignment 7: Cross-Site', 'Alice : Elgg For SEED Lab', and 'attacker32.com/addfriend.h'. The active tab is 'Alice : Elgg For SEED Lab', displaying the profile page for 'Alice' at 'www.seed-server.com/profile/alice'. The profile page includes a header with the site name 'Elgg For SEED Labs', a menu icon, and the name 'Alice'. Below the name are two buttons: 'Edit avatar' and 'Edit profile'. A profile picture of a blonde woman is shown. On the left, there is a sidebar with links for 'Blogs', 'Bookmarks', 'Files', and 'Pages'. An 'HTTP Header Live' extension window is open on the right, showing the headers for a POST request to 'http://www.seed-server.com/action/profile/edit'. The headers include Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Content-Type, Content-Length, Origin, Connection, Referer, Cookie, Upgrade-Insecure-Requests, and an Elgg token. The status bar at the bottom of the extension window shows 'POST: HTTP/1.1 302 Found' and 'Date: Thu, 21 Oct 2021 01:11:59 GMT'. The extension also has buttons for 'Clear', 'Options', 'File Save', and a checked 'Record Data' checkbox, with an 'autoscroll' option at the bottom.

Assignment 7: Cross-Site X Alice : Elgg For SEED Lab X attacker32.com/addfriend.h X

www.seed-server.com/profile/alice

Elgg For SEED Labs

Alice

Edit avatar Edit profile

Blogs

Bookmarks

Files

Pages

HTTP Header Live

http://www.seed-server.com/action/profile/edit

Host: www.seed-server.com

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv

Accept: text/html,application/xhtml+xml,application/xml

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: multipart/form-data; boundary=-----

Content-Length: 2964

Origin: http://www.seed-server.com

Connection: keep-alive

Referer: http://www.seed-server.com/profile/alice/edit

Cookie: system=PW; caf\_ipaddr=12.184.115.59; country=U

Upgrade-Insecure-Requests: 1

\_elgg\_token=oV6GHZB5N0p\_Lup4r6tWNw&\_elgg\_ts

POST: HTTP/1.1 302 Found

Date: Thu, 21 Oct 2021 01:11:59 GMT

Server: Apache/2.4.41 (Ubuntu)

Cache-Control: must-revalidate, no-cache, no-store, pr

expires: Thu, 19 Nov 1981 08:52:00 GMT

pragma: no-cache

Location: http://www.seed-server.com/profile/alice

Vary: User-Agent

Content-Length: 406

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

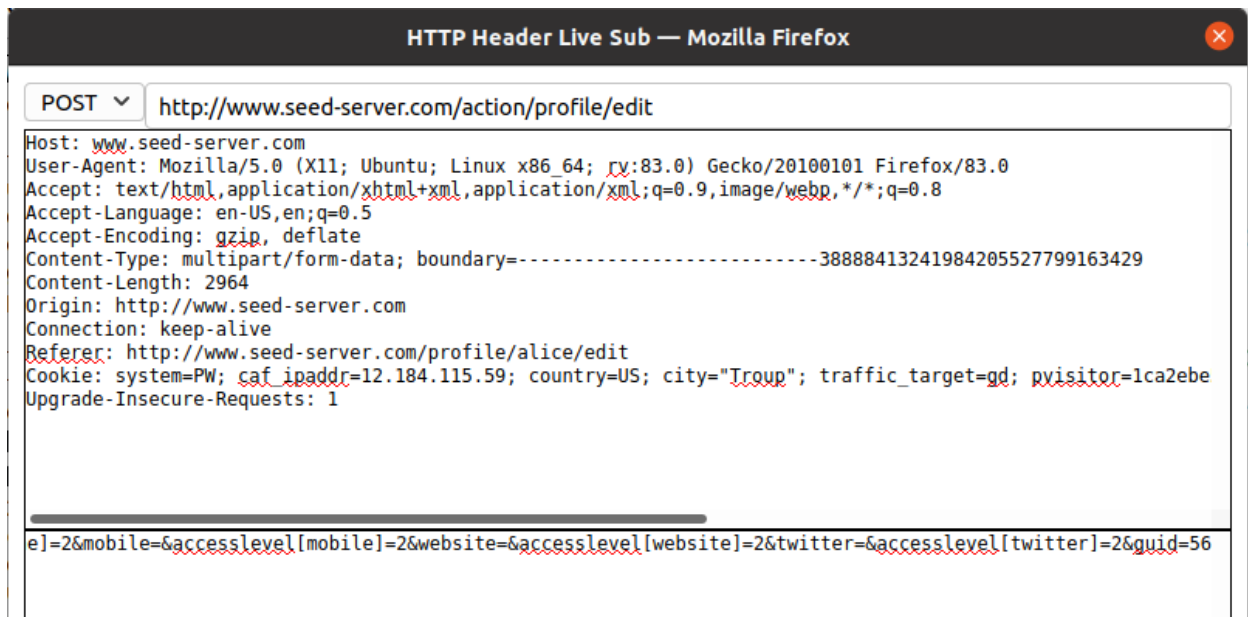
Content-Type: text/html; charset=UTF-8

http://www.seed-server.com/profile/alice

Clear Options File Save Record Data

autoscroll

In this task we use the HTTP header live to capture the post request that is generated when edit profile is saved



we get the guid from the post request's body which is 56 here



We are given the skeleton of the code for editing the profile as editprofile.html

We edit the .html file according to the details we have got from the previous steps

That is adding the value for name which is Alice, value for brief description which is "samy is my hero" and value for guid which is 56

We also change p.action to the url which is in the above post request

## Add blog post

**Title \***

alice please open this for free food


**Excerpt**

**Body \***

<http://www.attacker32.com/editprofile.html>

[Embed content](#) [Edit HTML](#)

**body p**

 **Samy**

- Blogs
- Bookmarks
- Files
- Pages
- Wire post

Then samy adds another post so that alice can open it and the attack can be executed

Assignment 7: Cross-Site X

alice please open this for X

CSRF Attacker's Page X

+

-

□


×

← → ↺ 🏠 🔒 [www.seed-server.com/blog/view/62/alice-please-op](http://www.seed-server.com/blog/view/62/alice-please-op) ... ☆ ⬇ 📄 📱 🔍 ⋮

**Elgg For SEED Labs** ≡

Samy › Blogs

# alice please open this for free food

 By **Samy** ⌚ a minute ago 🌐 Public 💬 👍

<http://www.attacker32.com/editprofile.html>

« Previous

**Comments**

[Embed content](#) [Edit HTML](#)

**B I U S I<sub>x</sub>**

**HTTP Header Live** ✕

```
http://www.attacker32.co
Host: www.attacker32.com
User-Agent: Mozilla/5.0 (X11;
Accept: text/html,application
Accept-Language: en-US,en;q=0
Accept-Encoding: gzip, deflat
Connection: keep-alive
Upgrade-Insecure-Requests: 1
NS_ERROR_NET_ON_WAITING_

http://www.attacker32.co
Host: www.attacker32.com
User-Agent: Mozilla/5.0 (X11;
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0
Accept-Encoding: gzip, deflat
Connection: keep-alive
Referer: http://www.attacker3
GET: HTTP/1.1 404 Not Fo
Date: Wed, 20 Oct 2021 22:39:
Server: Apache/2.4.41 (Ubuntu
Content-Length: 280
Content-Type: text/html; char

http://www.attacker32.co
Host: www.attacker32.com
```

Clear Options

File Save ☒ Record Data ☐

autoscroll

Then alice opens the malicious website by clicking on it

Alice

Edit avatar

Edit profile



Brief description  
Samy is my HERO!

Add widgets

Blogs

Bookmarks

Files

Pages

Wire post

Here we can see that when alice opens the malicious website the malicious javascript that exists in the .html (the forged post request send it to the malicious website) file gets executed and prints "samy is my hero" on alice's profile

Question1:

Boby can learn alice guid bu inspecting the add friend request on alice. The HTTP header live will give bob the url of the get request and he can fiend the id that alice used which will be alices guid

Question2:

This is not possible as bob will have to know the euid of the victim. Which means he cannot attack everyone and can attack only one person whose guid is known

Task4:

```
[10/20/21]seed@VM:~/.../Labsetup$ dockps
cddd82d871d0  elgg-10.9.0.5
4eff29ec5ec7  mysql-10.9.0.6
064bffe5de7  attacker-10.9.0.105
[10/20/21]seed@VM:~/.../Labsetup$ docksh cdd
root@cddd82d871d0:/# ls
bin  dev  home  lib32  libx32  mnt  proc  run  srv  tmp  var
boot  etc  lib  lib64  media  opt  root  sbin  sys  usr
root@cddd82d871d0:/# ls /var/www/elgg/vendor/elgg/elgg/engine/classes/Elgg/Security
Base64Url.php  Csrf.php  Hmac.php  HmacFactory.php  PasswordGeneratorService.php  UrlSigner.php
root@cddd82d871d0:/# cd /var/www/elgg/vendor/elgg/elgg/engine/classes/Elgg/Security
root@cddd82d871d0:/var/www/elgg/vendor/elgg/elgg/engine/classes/Elgg/Security#
```

Opening Csrf.php at it location

```
GNU nano 4.8                                Csrf.php                                Modified

/**
 * Validate CSRF tokens present in the request
 *
 * @param Request $request Request
 *
 * @return void
 * @throws CsrfException
 */
public function validate(Request $request) {
    // Return; // Added for SEED Labs (disabling the CSRF countermeasure)

    $token = $request->getParam('__elgg_token');
    $ts = $request->getParam('__elgg_ts');

    $session_id = $this->session->getID();

    if (($token) && ($ts) && ($session_id)) {
        if ($this->validateTokenOwnership($token, $ts)) {
            if ($this->validateTokenTimestamp($ts)) {
                // We have already got this far, so unless anything
                // else says something to the contrary we assume we're ok
                $returnval = $request->elgg()->hooks->trigger('action_gatekeeper',
                    'token' => $token,
                    'time' => $ts
                ], true);


                if ($returnval) {
                    [Cancelled]
                }
            }
        }
    }
}
```

Commenting out the return statement in in validation function to turn on counter measures

Elgg For SEED Labs

Samy > Blogs

alice please open this for free food

 By [Samy](#) 38 minutes ago Public

<http://www.attacker32.com/editprofile.html>

[« Previous](#)

Comments

Embed content Edit HTML

**B** *I* U ~~S~~ *I*<sub>x</sub>

HTTP Header Live

Clear

Options

File Save

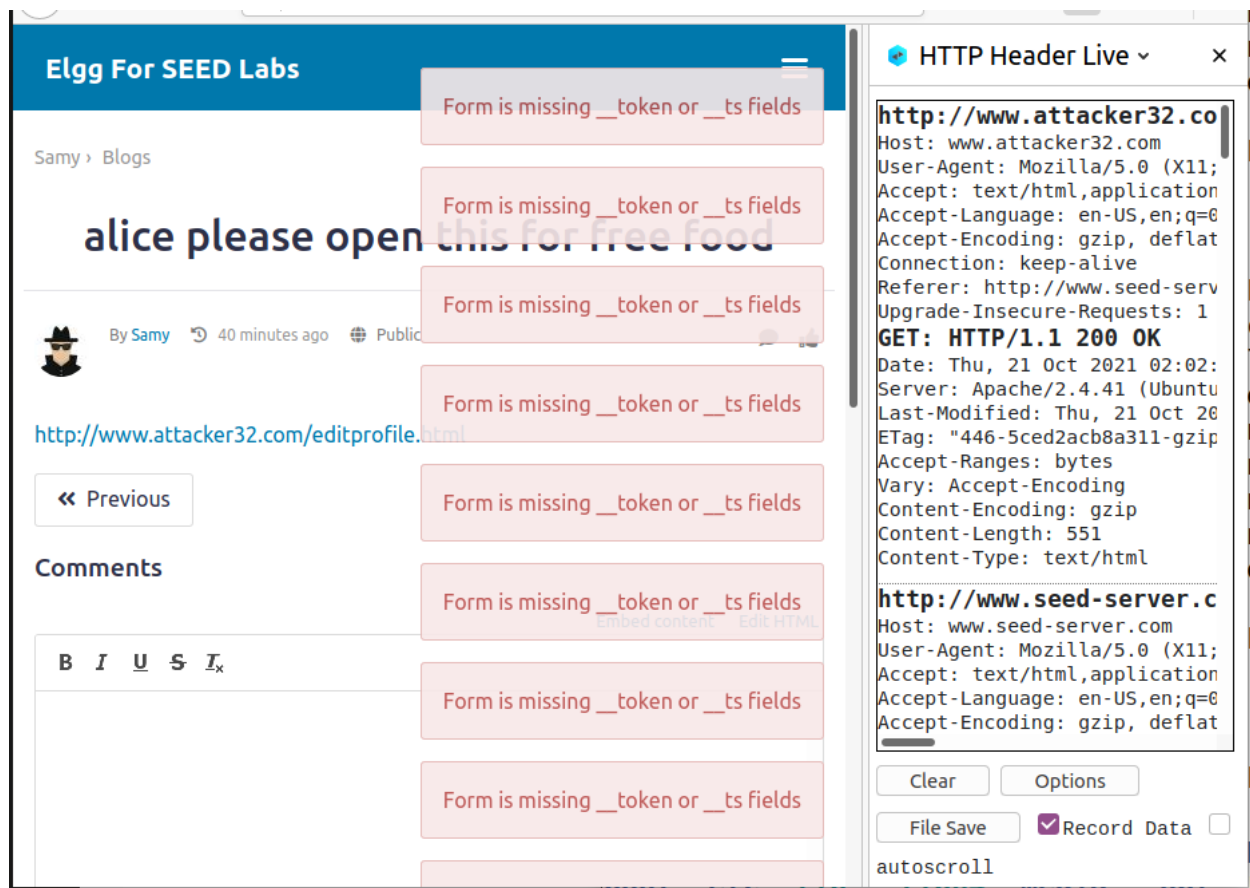
☒ Record Data ☐

autoscroll

here we try to do the same attack as in previous task



We are directed to the malicious webpage where we can't understand anything so we press the back button and go back to the elgg webpage



When we come back to the page we see there are multiple error messages on the screen as the counter measures are turned on and doesn't allow the attack to execute but the attack keeps running in background until it gets executed and because of the counter measure is turned on the attack can never execute as the token and ts values are missing